Oracle Payment Interface
Security Guide

Release 19.1
F14696-03
October 2023

Oracle Payment Interface Security Guide, Release 19.1

F14696-03

Contents

Preface

This document provides security reference and guidance for the Oracle Payment Interface (OPI).

Audience

This document is intended for:

- System administrators installing the Oracle Payment Interface
- End users

Customer Support

To contact Oracle Customer Support, access My Oracle Support at the following URL:
https://support.oracle.com

When contacting Customer Support, please provide the following:

- Product version and program/module name
- Functional and technical description of the problem (include business impact)
- Detailed step-by-step instructions to re-create
- Exact error message received and any associated log files
- Screenshots of each step you take

Documentation

Product documentation is available on the Oracle Help Center at
http://docs.oracle.com/en/industries/hospitality/

Revision History

Date	Description of Change
February 2019	Initial publication.
March 2019	Updated formatting and cover page with new template.
September 2019	Updated Payment Interface section that supports POS and PMS systems.
October 2023	Removed the MySQL 5.6 version across the document as the OPI installer no longer supports

1

Payment Interface Security Overview

This chapter provides an overview of Oracle Payment Interface security and explains the general principles of application security.

Basic Security Considerations

The following principles are fundamental to using any application securely:

- **Keep software up to date**. This includes the latest product release and any patches that apply to it.
- **Limit privileges as much as possible**. Users should be given only the access necessary to perform their work. User privileges should be reviewed periodically to determine relevance to current work requirements.
- **Monitor system activity**. Establish who should access which system components, and how often, and monitor those components.
- **Install software securely**. For example, use firewalls, secure protocols using TLS (SSL), and secure passwords. See Performing a Secure Payment Interface Installation for more information.
- **Learn about and use the Payment Interface security features**. See Implementing Payment Interface Security for more information.
- **Use secure development practices**. For example, take advantage of existing database security functionality instead of creating your own application security. See “Security Considerations for Developers” for more information.
- **Keep up to date on security information**. Oracle regularly issues security-related patch updates and security alerts. You must install all security patches as soon as possible. See the “Critical Patch Updates and Security Alerts” website: http://www.oracle.com/technetwork/topics/security/alerts-086861.html

Overview of Payment Interface Security

The Oracle Payment Interface (OPI) integrates with the Point-of-Sale (POS) and the Property Management Systems (PMS) to manage the connections with third-party payment service providers (PSP) and payment processors. It is an interface bridging POS/PMS and processors/partner PSP. It shields POS/PMS from credit card processing details and from details of interfacing with different payment terminals and processors/third-party payment service providers. It is a semi-integrated solution that can reduce or remove POS/PMS out of PADSS. It also provides a common platform that facilitates the adoption of new payment technologies/solutions.

The Oracle Payment Interface deploys on-premise with the POS and PMS client to transfer transaction data between the POS, PMS, and third-party payment service provider (PSP) hosts and terminals.

The following diagrams show how OPI bridges between POS/Opera and third-party PSPs for credit card processing.

Figure 1-1 Hosted Opera integrates with OPI and PSP

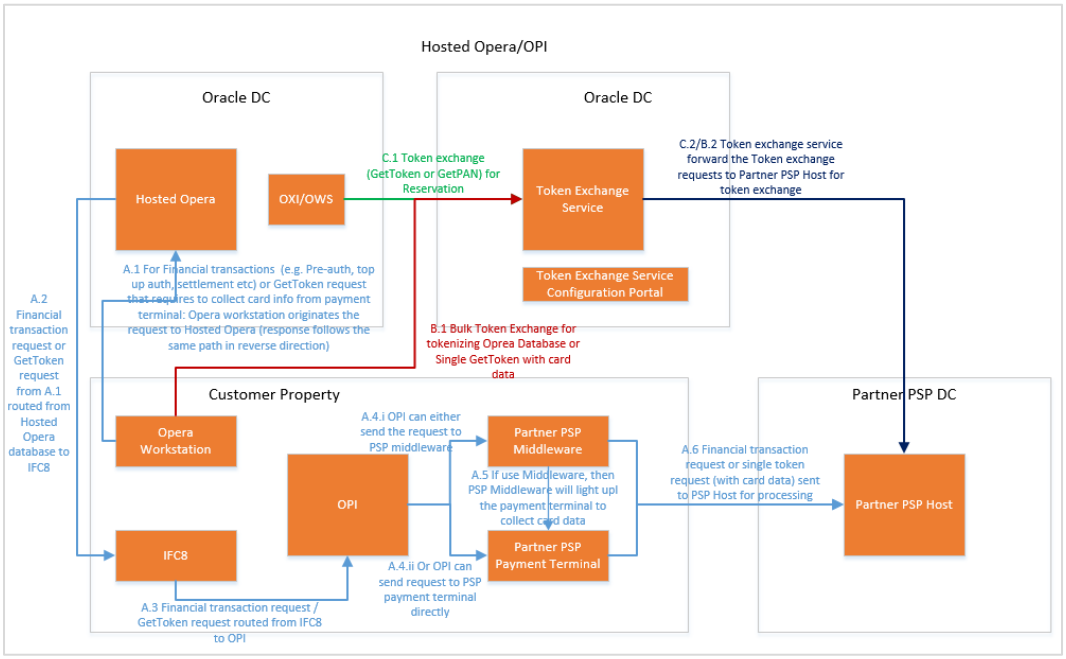


Figure 1-2 On Premise Opera integrates with OPI and PSP

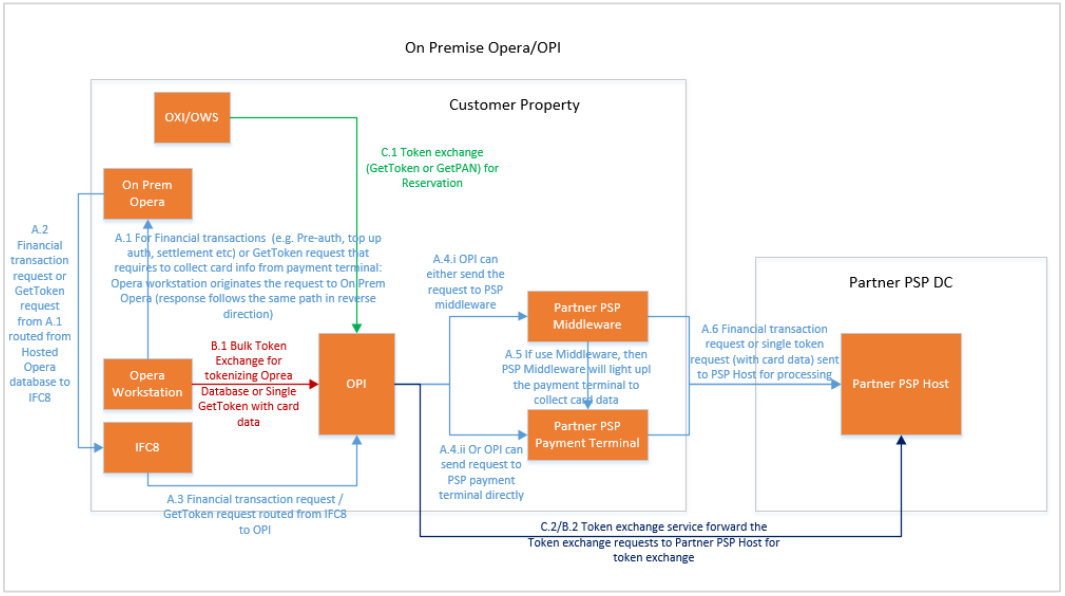
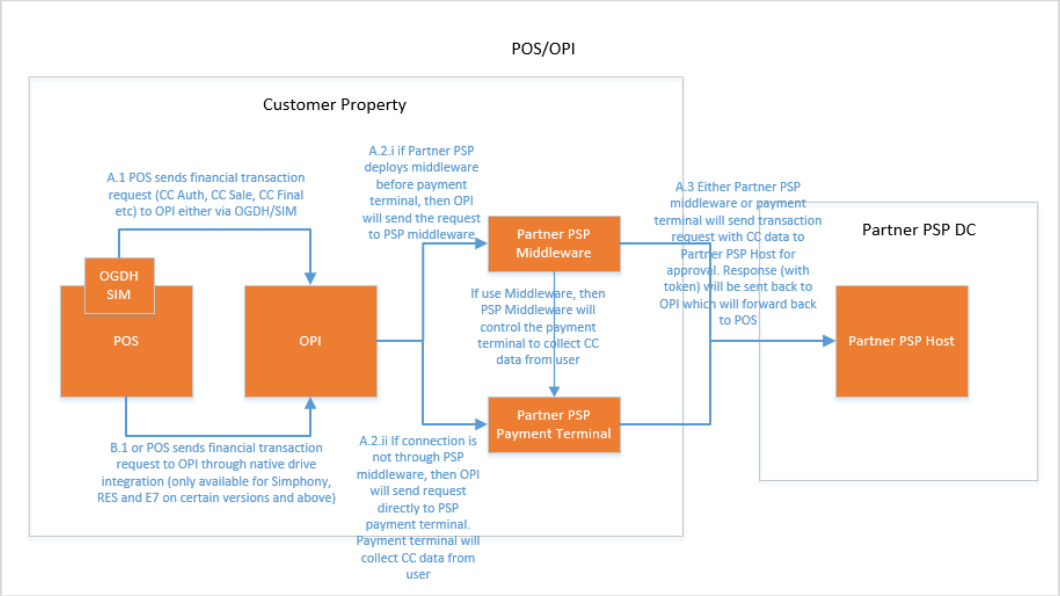
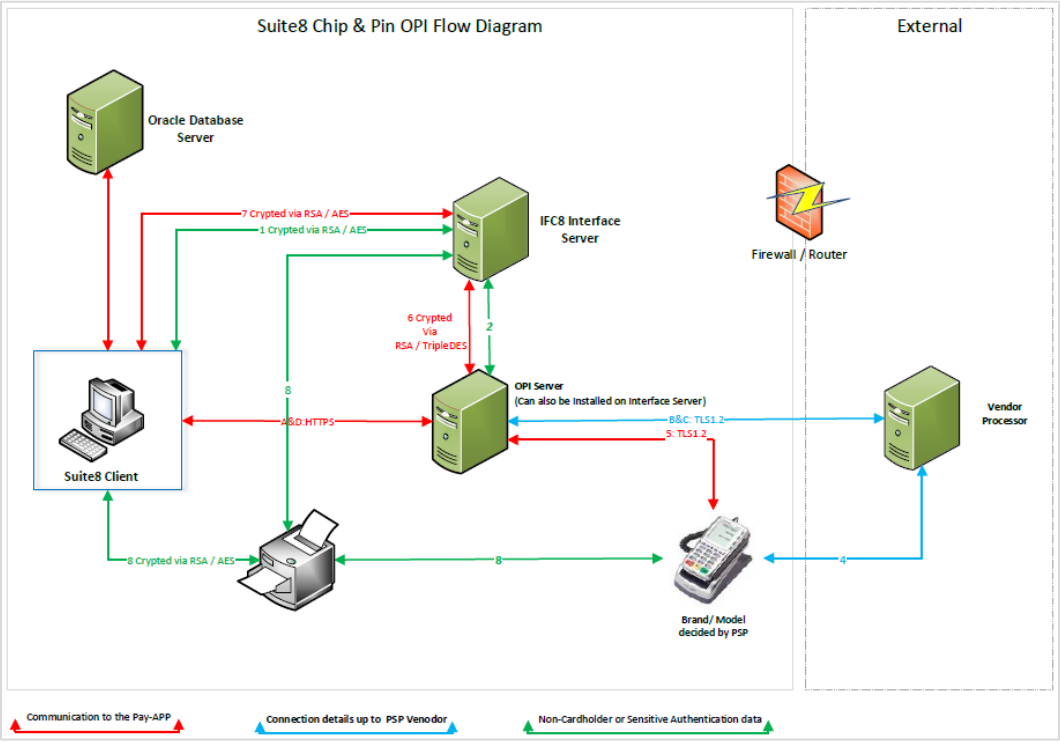


Figure 1-3 POS integrates with OPI and PSP



The following diagram depicts the connection from Suite8 to OPI TPS.

Figure 1-4 Suite8 Chip & Pin OPI Lan-token



Transactional flow:

1. Suite8 sends only payment request to interface. No card data.

2. Interface (IFC8) forwards payment request to OPI

3. OPI forward request to Pin Pad via TSL 1.2

4. Vendor will process request including prompting for card and communication with acquirer.

5. Pin Pad send response to OPI via TSL 1.2

6. OPI provides final response to Suite8

7. Suite8 saves transaction number / auth code, card token and last 4 digits of PAN received from vendor

8. Optional. Suite8 / Interface (IFC8) prints CC receipt provided by Vendor, Mask CC data up to vendor

Process Get Token for entered PAN:

A: Optional: Suite8 client sends PAN to OPI to request token

B & C: OPI connects to Vendor requesting token. OPI receives token & last 4 PAN digits from vendor

D: OPI sends back response with token to Suite8 client. Suite8 saves token, last 4 digits of PAN encrypted in DB

Establishing Secure Connections

- The Property Management System (PMS) Hosted or On Premise both use IFC8 to connect with OPI. IFC8 provides a shared key protected mechanism to secure the connection.
- PMS uses HTTPS with TLS 1.2 to connect to OPI for Token Exchange Services.
- POS has two ways to connect to OPI depending on what type of interface is between POS and OPI. POS systems with OGDH use HTTPS with TLS 1.2 to connect to OPI and POS systems with the native driver use HTTP with encrypted data to connect to OPI.
- OPI uses HTTPS with TLS 1.2 to connect to PSP with an option of two-way authentication for financial transactions.
- OPI uses HTTPS with TLS 1.2 to connect to PSP with two-way authentication for Token Exchange Services.
- The OPI Configuration Tool and Wizard use HTTP with encrypted data to connect to the OPI Configuration Service.

Recommended Deployment Configurations

The Oracle Payment Interface (OPI) deploys on-premise with the POS and the PMS. The Oracle Payment Interface service deploys as a Microsoft Windows Service and listens to a configurable port for requests. System/merchant administrators can use the OPI

Configuration Tool (a Microsoft Windows application) to configure the Oracle Payment Interface service. A configuration service is also available for client applications such as POS and PMS to configure OPI. The Oracle Payment Interface service uses Java KeyStore to save the communication certificates.

PII Data Security

Personally identifiable information (PII) is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context.

OPI only collects minimal data (first name, last name) for the person who is assigned to manage the configuration. The OPI Configuration Tool provides a user profile page which shows the user's information in the system and allows the user to update/delete the information. Starting with OPI 19.1, PII data is saved as encrypted data in the database. The encryption algorithm is AES 256.

The transaction data is automatically purged after the configurable retention period. The user account profile data can be deactivated by the system administrator. To maintain the integrity of the audit trail, the deactivated user can be permanently removed from the database only after a configurable retention period. Note the user account profile data is very limited (first name, last name) and only limited to users who are assigned responsibility to manage the configuration. Once purged, the data cannot be re-created, accessed, or read.

Based on the secure connection from POS/PMS to OPI and OPI to PSP, PII data is encrypted during the process of communication.

Tokenization is always enabled by OPI 19.1 to protect user credit card information.

Component Security

Oracle Database Security

See the *Oracle Database Security Guide*.

2

Performing a Secure Payment Interface Installation

This chapter describes how to plan for installing the Oracle Payment Interface.

See the *Oracle Payment Interface Installation Guide* for more information and instructions.

Pre-Installation Configuration

Before you install the Oracle Payment Interface, you must complete the following tasks:

- Apply critical security patches to the operating system.
- Apply critical security patches to the database server application.
- Install Microsoft .Net Framework. You must install Microsoft .Net Framework release 4.0.30319 or higher.
- Install Java Runtime Environment (JRE), version 1.8 or above
- Install Database Server, the databases OPI 19.1 supports are
  - MySQL 5.7
  - SQL Server 2008 R2 or later
  - SQL Server Express 2008 R2 or later
  - Oracle 12c or later
- Confirm database root /system administrator's password follows the Oracle GIS Guidelines and contains:
  - At least 8 characters
  - 1 letter
  - 1 number
  - 1 special character !@#$%^&*
- Confirm the memory size contains at least 1024 MB of free space exclusively for OPI to use.
- Confirm the hard drive disk space contains at least 6 GB of free space exclusively reserved for OPI.

Payment Interface Installation

See the *Oracle Payment Interface Installation Guide* for more information and instructions.

Configuring the Connection

When integrating an Oracle Hospitality POS with the native driver, the Oracle Payment Interface Service installer requests a POS key or passphrase to authenticate the POS connection request from the native POS driver. This passphrase must contain at least 15 characters with at least one alphabet, one special character, and one number character.

The following Oracle Hospitality POS systems support connecting using a native driver:

- Simphony release 2.10.2 or higher
- RES 3700 release 5.5 MR1 or higher

When connecting to the Oracle Hospitality POS with an OGDH connection, during the installation process you must configure a POS certificate password when setting up a property. The POS certificate password must follow the Oracle GIS guidelines. The following systems support the use of OGDH connection:

- Simphony release 2.7 MR4 or higher
- Simphony First Edition release 1.6 MR6 or higher
- RES 3700 release 5.0 or higher
- 9700 Point-of-Sale release 4.0 or higher

For POS, it is recommended to use the native driver, if supported.

When connecting to PMS, during the installation process you must create a key to secure the communication to IFC8. You must also input the key to the PMS IFC8 configuration. The following Oracle Hospitality PMS systems support connecting to the Oracle Payment Interface:

- OPERA On Premise 5.5.24.4 or higher
- OPERA V5 Hosted 5.5.25 or higher
- OPERA V5.6.4 or higher
- OPERA Cloud 1.20.16 or higher
- OPERA Cloud 19.2 or higher
- Suite8 8.12.0.0 and higher

The OPI on-premise Token Exchange requires three sets of certificates for HTTPS communications (Refer to the OPI Installation Guide for details on how to deploy certificates). It is highly recommended to use CA-signed certificates.

- OPI > PSP - (PSP - Client Side Certificate)
- OPI > PSP - (PSP – Server’s Root Certificate)
- Opera > OPI - (OPI- Server Side Certificate)

Post-Installation Configuration

This section describes additional security configuration steps to complete after you install the Oracle Payment Interface.

Applying Software Patches

Apply the latest Oracle Payment Interface patches available on My Oracle Support.

Follow the installation instructions included with the patch.

Configuring the Oracle Payment Interface Service

During the installation, the Oracle Payment Interface Configuration Wizard launches to configure the Oracle Payment Interface Service. You can access the Configuration Wizard manually to add or update connections after the installation. Refer to the Oracle Payment Interface Installation Guide for instructions.

OPI provides an optional feature to communicate with the PSP using two-way authentication. In this case, OPI communicates to the PSP using HTTPS with a client certificate for client authentication. That is, while a server-side certificate is expected to be deployed at the PSP (server-side) for HTTPS communication, the PSP is also expected to provide a client-side certificate to be deployed at the OPI side. OPI will present this client certificate during HTTPS communication with the PSP so that the PSP can authenticate OPI properly. Refer to the Oracle Payment Interface Installation Guide for the detailed certificate handling steps.

In order to achieve this, the PSP must provide two files:

- A client-side certificate file with file type .pfx. This is a PKCS#12 Certificate file that contains a public key and a private key and will be protected by a password.
- The root certificate file for the server-side certificate that is deployed at the PSP side. OPI needs to load this root certificate file into the Java Key store so that OPI can properly recognize and trust the server-side certificate deployed at the PSP side. The root certificate file provided by the PSP should be in .cer or .crt format.

Rotating the Keys and Passphrases that Protect Communications

System administrators must update the password and rotate the POS key frequently by following the PCI Guidelines for rotating encryption keys.

To rotate the POS key for POS with native driver:

1. Open the OPI Configuration Tool.
2. Go to **POS Configuration** tab to update the key.

To rotate the shared security key for PMS IFC8:

1. Run the configuration wizard to recreate the key.
2. Update PMS IFC8 configuration to have the new key.

To rotate the shared passphrase between the OPI configuration service and tools:

1. On the OPI installation directory, go to the \\OraclePaymentInterface\v19.1\Services\ConfigService directory
2. Run `LaunchSettingsAdminTool.bat` as administrator, select **Configuration Passphrase** Tab, and then **Update Passphrase**.
3. Go to the \\OraclePaymentInterface\v19.1\Configdirectory.
4. Run `RotatePassphrase.bat` as administrator, and then **Update Passphrase** for the tool.

The expiration date for the PSP client-side certificates (for both financial transactions and token proxy service) will vary depending on what the PSP set during creation of the certificate. Check the expiration date in the properties of the certificate files. **To avoid downtime to the interface you must update the PSP certificates prior to the expiration date.**

Purging Data

Audit data, logs, and transaction records save to the database. Purge data according to the merchant's contract policy.

3

Implementing Payment Interface Security

Oracle Payment Interface Service Security

Managing Users

The OPI Configuration Tool and the Wizard both have a user/password mechanism for authentication and authorization. The SuperUser is created when the configuration service is installed. Other users can be created/viewed/updated by the Configuration Tool. Ensure all passwords follow Oracle GIS guidelines.

The user account profile data can be deactivated by the system administrator. To maintain the integrity of the audit trail, the deactivated user can be permanently removed from the database only after a configurable retention period. Once purged, the data cannot be re-created, accessed, or read.

Authenticating the Service

Authentication means verifying the identity of a user, device, or other entity who wants to use data, resources, or applications. Validating that identity establishes a trust relationship for future interactions and applies to the entity accessing the service and to the entity providing the service.

In this release, the native POS driver communicates from the POS to Oracle Payment Interface using a shared passphrase to generate a Server Key encrypting the communication between client and server. Only the server/client which has the shared passphrase configured is an authenticated server/client.

PMS IFC8 communication channel uses a shared key to authenticate server and client.

OPI Configuration Service and Tools communicate each other with shared key to authenticate server and clients.

Opera and On-Premise TPS use basic HTTP username/password authentication on top of HTTPS with TLS 1.2.

Backup and Recovery

The OPI 19.1 Configuration Tool lets you export the OPI configuration to an XML file and import to another OPI instance. The configuration to be exported does not contain security information, like passphrases, shared security keys, etc. Once a set of configuration has been imported, the administrator can use the Configuration Tool to reset security data.

For more information about system backup and recovery, refer to the following bulletins on My Oracle Support:

- Oracle Payment Interface Recovery Plan - SQL Edition (Doc ID 2479372.1)

- Oracle Payment Interface Recovery Plan - Oracle Database Edition (Doc ID 2470207.1)
- Oracle Payment Interface Recovery Plan - MySQL Edition (Doc ID 2414504.1)

Audit Trail Logging

When a user makes changes to Oracle Payment Interface settings, the changes save in the database. Using the OPI Configuration Tool, system administrators can review, filter, and purge audit log records. For security, no audit log information shows in the debug log files.

Purging Audit Trail Data
The audit records save in the database for a minimum of 90 days. You can manually purge the records older than 90 days using the Configuration Tool. Once purged, the data cannot be re-created, accessed, or read.

To purge Audit records:

1. Log in to the OPI Configuration Tool as a system administrator.
2. Go to the **Audit** page.
3. Select the **Start Date** and **End Date** to view the audit record.
4. Select **View** to view the records for the selected date range.
5. Select **Purge** to purge the Audit records.

Appendix A
Secure Deployment Checklist

This appendix lists actions that need to be performed to create a secure system. The following is an example:

The following security checklist includes guidelines that help secure your database:

- Install only what is required.
- Enforce password management.
- Practice the principle of least privilege.
  - Grant necessary privileges only.
  - Revoke unnecessary privileges from the PUBLIC user group.
  - Restrict permissions on run-time facilities.
- Restrict network access.
- Apply all security patches and workarounds.
  - Use a firewall.
  - Never poke a hole through a firewall.
  - Protect the Oracle listener.
  - Monitor listener activity.
  - Monitor who accesses your systems.
  - Check network IP addresses.